対話型 AI を使ってみる
その問題点と課題を探る

JCA-NET セミナー

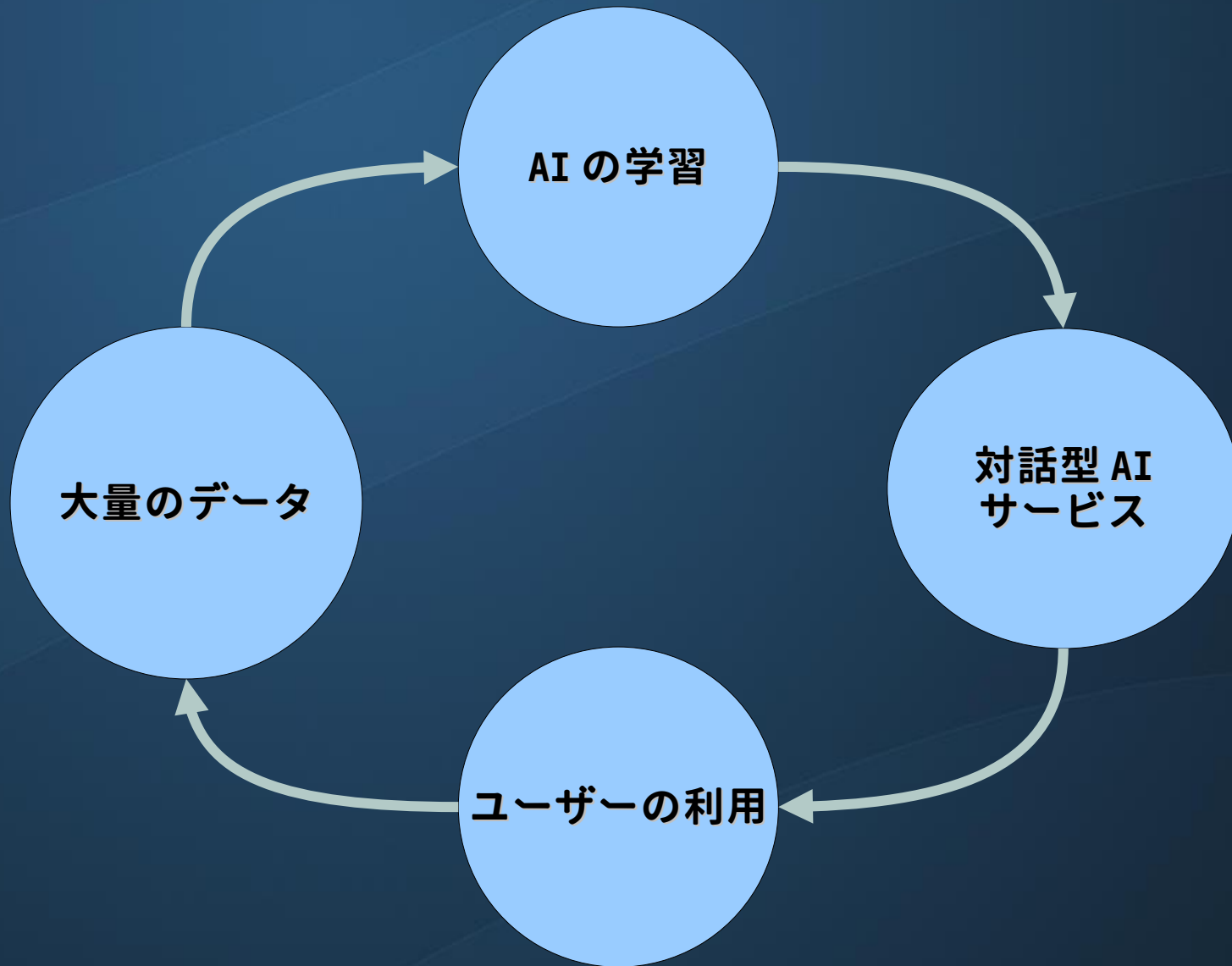
2024 年 11 月 19 日

小倉利丸

toshi@jca.apc.org

対話型 AI を使ってみる
その問題点と課題を探る

Google や Microsoft などが検索サービスに対話型 Ai が導入しはじめており、検索のスタイルが大きく変わりつつあります。19 日のセミナーでは、この AI 検索の問題をとりあげます。 これまでもセミナーでは、 Google での検索のプライバシーリスクを指摘してきましたが、対話型 AI の普及でプライバシーリスクは更に高まる可能性があります。他方で、これまでもプライバシーを重視する DuckDuckGo などを検索に使うことを推奨してきましたが、この DuckDuckGo もまた対話型 AI(AI Chat) を導入しはじめています。今回のセミナーでは、プライバシー重視の DuckDuckGo が導入した対話型 AI を実際に使いながら課題を探ります。

対話型 AI を使ってみる
その問題点と課題を探る

対話型 AI を使ってみる
その問題点と課題を探る

DuckDuckGo の対話型 AI(AI Chat) の仕組み

- DuckDuckGo は幾つかの対話型 AI を提供するサービスとユーザーとの間を仲介する
- DuckDuckDo は、ユーザーの質問内容、ユーザーがネットにアクセスすることで晒す様々なプライバシーデータ (IP アドレス、位置情報、使用パソコンなど) を削除した上で、質問を対話型 AI サービス業者に渡す
- DuckDuckGo は、対話型 AI の技術的な仕組みを全て把握できているわけではない
- 回答の正確性などを DuckDuckGo が独自に修正できるわけではない

GPT-4o mini

Claude 3 Haiku

Llama 3.7

Mixtral 8x7B

対話型 AI 提供企業

ユーザーはこのうちからひとつを選択して利用する

質問からプライバシー情報を削除

DuckDuckGo 対話型 AI サービス

質問

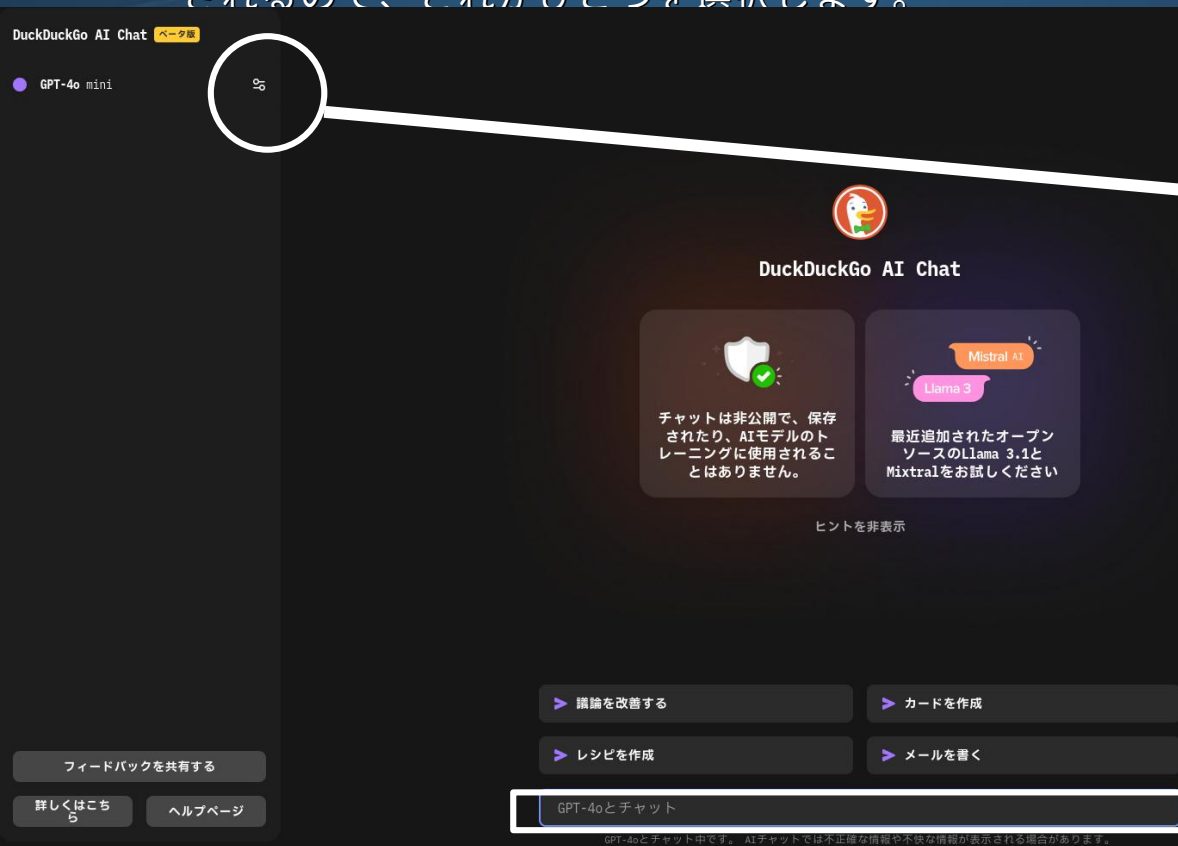
ユーザーの利用

対話型 AI を使ってみる
その問題点と課題を探る

DuckDuckGo の対話型 AI は下記から使うことができます。

- 下記にアクセスします

https://duckduckgo.com/

- 右脇のサイドメニューを開き、 AI Chat というメニューをクリックすると下左図のようなページになります。左メニューの脇にある選択アイコンをクリックすると下右図のように使用する AI の選択肢が示されるので、どれかひとつを選択します。

対話型 AI を使ってみる
その問題点と課題を探る

- 一般に回答には、その根拠となるデータ (参考資料や典拠など) は示されません。
- 意識的に、「その回答の根拠となる資料の URL を教えてください」などと質問する必要があります。
- 回答が明らかに間違いである場合は判断がつきますが、そうではない場合 (自分が十分な予備知識がない場合など) 間違いに気づかないことがありえます。
- 質問への回答が、あたかも唯一の回答であるかのように示される場合があります。「その回答の他に、どのような回答がありますか」などと意識的に追加の質問をする必要があります。

対話型 AI を使ってみる
その問題点と課題を探る

- 一般に、従来型の検索では、複数のサイトを表示し、そのなかからユーザー側が選択して、必要な「答え」を探す、という行動をとるために、ユーザー側の選択の意思が働きます。そうであっても、並び順が、ユーザーの選択に大きな影響をもたらします。
- 対話型 AI は、複数の回答を並列して示すことが少なく、利用者によっては、その答えを唯一絶対正しい答えだとして無批判に受け入れ易い仕組みになっています。
- 回答に異論がある場合、コンピュータに対して反論するということはどのようなことなのか、明確な方法論が確立していません。結果として、あたかも人間と議論しているかの錯覚に陥る危険性があります。

対話型 AI を使ってみる
その問題点と課題を探る

DuckDuckGo の対話型 AI は、直接 AI サービスを利用するよりもプライバシーへの配慮がある分、安心できると思いますが、完全にプライバシーが防御されるわけではありません。

使うのか、使わないのかも含めて、対話型 AI をどうすべきかは、今後も継続した議論が必須です。